Homework 3

Mark Schulist

1)

Show that $61 \in (\mathbb{Z}/159\mathbb{Z})^{\times}$. Same as showing $(61, 159) = 1$.

$$\begin{aligned} 159 &= 2 \cdot 61 + 37 \\ 61 &= 37 + 24 \\ 24 &= 13 + 11 \\ 11 &= 2 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0 \end{aligned} \tag{1}$$

So $(61, 159) = 1$.

Now find the inverse of 61 in $\operatorname{mod} 159$.

$$\begin{aligned} 61 \cdot z \equiv 1 \operatorname{mod} 159 \\ 61 \cdot z + 159k = 1 \end{aligned} \tag{2}$$

Use extended Euclidean to find k and z.

$$\begin{aligned} 1 &= 11 - 2 \cdot 5 \\ &= 11 - 5(13 - 11) \\ &= 11 - 5 \cdot 13 + 5 \cdot 11 \\ &= 6 \cdot 11 - 5 \cdot 13 \\ &= 6(24 - 13) - 5 \cdot 13 \\ &= 6 \cdot 24 - 13 \cdot 6 - 5 \cdot 13 \\ &= 6 \cdot 24 - 11 \cdot 13 \\ &= 6 \cdot 24 - 11(37 - 24) \\ &= 6 \cdot 24 - 11 \cdot 37 + 11 \cdot 24 \\ &= 17 \cdot 24 - 11 \cdot 37 \\ &= 17(61 - 37) - 11 \cdot 37 \\ &= 17 \cdot 61 - 17 \cdot 37 - 11 \cdot 37 \\ &= 17 \cdot 61 - 28 \cdot 37 \\ &= 17 \cdot 61 \cdot 28(159 - 2 \cdot 61) \\ &= 17 \cdot 61 - 28 \cdot 159 + 56 \cdot 61 \\ &= \underbrace{73}_{z} \cdot 61 \underbrace{-28}_{k} \cdot 159 \end{aligned} \tag{3}$$

So $61^{-1} = 73$ in $\mathbb{Z}/159\mathbb{Z}$.

2)

p is prime. Show that $\phi(p^n) = p^{n-1}(p - 1)$.

Proof. Because p is prime, we know that $\phi(p) = p - 1$. In the number system $\mathbb{Z}/p^n\mathbb{Z}$, there are $\frac{p^n}{p} = p^{n-1}$ numbers that share a factor with p^n (the multiples of p). So we need to subtract those from the total quantity of numbers in this number system, which gives us $p^n - p^{n-1}$ numbers that are coprime to p^n. Hence, $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p - 1)$. □

3)

3.a)

We need to create a bijection between $(\mathbb{Z}/m\mathbb{Z})_e$ and $(\mathbb{Z}/d\mathbb{Z})^\times$. We know $d \mid m, m = de$.

$$\begin{aligned} f : (\mathbb{Z}/m\mathbb{Z})_e &\to (\mathbb{Z}/d\mathbb{Z})^\times \\ f(x) &= ex \end{aligned} \tag{4}$$

We can show that f is injective. Suppose $f(x_1) = f(x_2)$. Then

$$\begin{aligned} ex_1 &= ex_2 \\ dex_1 &= dex_2 \\ mx_1 &= mx_2 \\ x_1 &\equiv x_2 \bmod m \end{aligned} \tag{5}$$

Now we show that f is surjective. We need to show that given any $y \in (\mathbb{Z}/d\mathbb{Z})^\times$, we can find an $x \in (\mathbb{Z}/m\mathbb{Z})_e$ such that $f(x) = y$.

We know that for any $y \in (\mathbb{Z}/m\mathbb{Z})_e$, $(y, m) = e$. Hence $(y, de) = e$ and $(y, d) = 1$ as all common factors must come from e. This means that $y \in (\mathbb{Z}/d\mathbb{Z})^\times$, and because $e \mid y$ and $m = de$, we know that $ye^{-1} \in (\mathbb{Z}/d\mathbb{Z})^\times$.

So the (two-sided) inverse of f is $f^{-1}(y) = ye^{-1} \in (\mathbb{Z}/d\mathbb{Z})^\times$.

3.b)

We want to show that $m = \sum_{d \mid m} \phi(d)$.

Proof. Given an $a \in (\mathbb{Z}/m\mathbb{Z})_e$, then we know that a is only in this particular set, and no other. If e changes value, then a will no longer be in the set. This is because (m, a) is fixed and will only equal one e.

Hence all of the $(\mathbb{Z}/m\mathbb{Z})_e$ sets (for all possible e) will be pairwise disjoint.

Because they are all pairwise disjoint (they partition the set of all values in $\mathbb{Z}/m\mathbb{Z}$), the union of all $(\mathbb{Z}/m\mathbb{Z})_e = \mathbb{Z}/m\mathbb{Z}$. We can show this is true by showing containment in both directions.

First show that $\mathbb{Z}/m\mathbb{Z} \subset \bigsqcup (\mathbb{Z}/m\mathbb{Z})_e$. Suppose we have an $\alpha \in \mathbb{Z}/m\mathbb{Z}$. Then $\alpha \in (\mathbb{Z}/m\mathbb{Z})_e$ for the value of e that makes $(\alpha, m) = e$. We know that there exists an e where this is true because we are taking the union over all possible values of e (the factors of m).

Now we show that $\bigsqcup (\mathbb{Z}/m\mathbb{Z})_e \subset (\mathbb{Z}/m\mathbb{Z})$. For any $\beta \in (\mathbb{Z}/m\mathbb{Z})_e$, we know that $\beta \in \mathbb{Z}/m\mathbb{Z}$ as β must be in the set $\{0, 1, ..., m - 1\}$ which is the same as $\mathbb{Z}/m\mathbb{Z}$.

Hence:

$$
\begin{aligned}
&\bigsqcup_{e} (\mathbb{Z}/m\mathbb{Z})_e = \mathbb{Z}/m\mathbb{Z} \\
\implies &\sum_{e} |(\mathbb{Z}/m\mathbb{Z})_e| = m
\end{aligned} \tag{6}
$$

We know that $(\mathbb{Z}/d\mathbb{Z})^\times \rightsquigarrow (\mathbb{Z}/m\mathbb{Z})_e$ and that $\phi(d) = |(\mathbb{Z}/d\mathbb{Z})^\times|$. Therefore, if we add $\phi(d)$ for all d that divide m, we will get the same value as adding $|(\mathbb{Z}/m\mathbb{Z})_e|$ for all e, which is the same as m.

Hence:

$$
m = \sum_{d \mid m} \phi(d) \tag{7}
$$

□

4)

Given p is an odd prime, show that

$$
\begin{aligned}
1^2 \cdot 3^2 \cdot \ldots \cdot (p-2)^2 &\equiv (-1)^{\frac{p+1}{2}} \bmod p \\
2^2 \cdot 4^2 \cdot \ldots \cdot (p-1)^2 &\equiv (-1)^{\frac{p+1}{2}} \bmod p
\end{aligned} \tag{8}
$$

Proof. We can start with the odd case. By the definition of squaring numbers, we can rewrite the LHS as:

$$
(1 \cdot 3 \cdot 5 \cdot \ldots \cdot (p-2))(1 \cdot 3 \cdot 5 \cdot \ldots \cdot (p-2)) \tag{9}
$$

And then further rearranage as shown below, using the fact that $-p(-a) \equiv a \bmod p$.

$$
(1 \cdot 3 \cdot 5 \cdot \ldots \cdot (p-2))((-1)(p-1) \cdot (-1)(p-3) \cdot \ldots \cdot (-1)4 \cdot (-1)2) \tag{10}
$$

We can group the terms together to get in a form where we can apply Wilson's Theorem.

$$
\begin{aligned}
\underbrace{(1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2)(p-1)))}_{-1}(-1)^{\frac{p-1}{2}} &\equiv (-1)^{\frac{p-1}{2}}(-1) \bmod p \\
&\equiv (-1)^{\frac{p+1}{2}} \bmod p
\end{aligned} \tag{11}
$$

The even case is nearly identical:

$$
\begin{aligned}
(2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-3)(p-1))((-1)(p-2) \cdot (-1)(p-4) \cdot \ldots \cdot (-1)3 \cdot (-1)1) &\equiv (-1)^{\frac{p-1}{2}}(-1) \\
&\equiv (-1)^{\frac{p+1}{2}}
\end{aligned} \tag{12}
$$

□

5)

p is an odd prime.

5.a)

Show that $x^2 = 0$ has one solution in $\mathbb{Z}/p\mathbb{Z}$.

Proof. We know that a^2 has an inverse if and only if $a^2 \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. We are given that $a^2 \equiv 0 \bmod p$, so a does not have an inverse. Because a^2 does not have an inverse, the only way to get $a^2 = 0$ is if $a = 0$, which is the single solution. □

5.b)

$a \in (\mathbb{Z}/p\mathbb{Z}), a \in \{1, ..., p-1\}$. We want to show that if $x^2 = a$ has a solution mod p, then it has exactly 2 solutions.

Proof. We can first show that x has at least 2 solutions.

If x is a solution to $x^2 \equiv a$, then $p - x$ is also a solution.

$$(p-x)^2 = p^2 - 2px + x^2 \equiv x^2 \bmod p = a \tag{13}$$

Now we show that if there is a solution, there are only 2 solutions.

Assume that $y \neq x$ and $x^2 = y^2$. Then

$$\begin{aligned} x^2 - y^2 &= 0 \\ (x+y)(x-y) &= 0 \\ y \neq x \Longrightarrow \quad x + y &= 0 \\ y &= p - x \end{aligned} \tag{14}$$

Which is the other solution. This means that if we are given one solution, the only possible other solution is the one we showed above in Equation 13. □

5.c)

$a \in (\mathbb{Z}/p\mathbb{Z})^\times$ is square if $\exists b \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $b^2 = a$.

Show that half of the elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ are squares.

$$\begin{aligned} f &: (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \\ f(x) &= x^2 \end{aligned} \tag{15}$$

For all $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, $x^2 = (p-x)^2$. Therefore, there are two elements in the domain that get mapped to each element in the codomain.

Because the domain and codomain have the same size $\phi(p) = p - 1$, we can only *hit* half of the elements in the codomain (both the domain and codomain are finite), meaning that the size of the image $f = \frac{p-1}{2}$.

5.d)

$$(\mathbb{Z}/7\mathbb{Z})^\times = \{1, 2, 3, 4, 5, 6\} \tag{16}$$

The squares are $\{1, 2, 4\}$ (by squaring each element in the above set and seeing where it lands).

5.e)

$$(\mathbb{Z}/15\mathbb{Z})^\times = \{1, 2, 4, 7, 8, 11, 13, 14\} \tag{17}$$

The squares are $\frac{2}{8}$ of the original elements, less than the 0.5 if we were working in a prime modulo.

6)

6.a)

$$A = \begin{bmatrix} 5 & 5 \\ 2 & 7 \end{bmatrix} \tag{18}$$

$$ad - bc = 25 \tag{19}$$

Now find the inverse of 25 in mod 9.

$$\begin{aligned} 25x &\equiv 1 \bmod 9 \\ 4 \cdot 25x &\equiv 4 \bmod 9 \\ x &\equiv 4 \bmod 9 \end{aligned} \tag{20}$$

$$\begin{aligned} A^{-1} &= 4\begin{bmatrix} 7 & -5 \\ -2 & 5 \end{bmatrix} \\ &= \begin{bmatrix} 28 & -20 \\ -8 & 20 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 7 \\ 1 & 2 \end{bmatrix} \end{aligned} \tag{21}$$

6.b)

$$\begin{aligned} \begin{bmatrix} 5 & 5 \\ 2 & 7 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 1 \\ 8 \end{bmatrix} \\ \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 1 & 7 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 1 \\ 8 \end{bmatrix} \\ \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 57 \\ 17 \end{bmatrix} \\ \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 3 \\ 8 \end{bmatrix} \end{aligned} \tag{22}$$

6.c)

$m = 26, n = 3$

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 3 \\ 3 & 5 & 3 \end{bmatrix} \tag{23}$$

$$b = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \tag{24}$$

I wrote the following code to compute the Hill Cipher. It finds the numeric value of the characters and goes 3 characters at a time, multiplying A by the vector of characters and adding b.

```
def encrypt_word(word: str, func: callable):
    res = ""
```

```
    for i in range(len(word) // 3):
        chars = word[i * 3 : i * 3 + 3]
        numeric_chars = np.array([ord(c) - 97 for c in chars])
        encrypted_numeric = func(numeric_chars)
        encrypted_chars = [chr(num_char + 97) for num_char in encrypted_numeric]
        for c in encrypted_chars:
            res += c

    return res

def f(x: np.ndarray):
    A = np.array(
        [
            [1, 2, 3],
            [0, 4, 3],
            [3, 5, 3],
        ]
    )
    b = np.array([1, 2, 3])

    return (A @ x + b) % 26

encrypt_word("banana", f)
```

This returns `pptbcq`.

6.d)

I computed A^{-1} and here is the result.

$$A^{-1} = \begin{bmatrix} 15 & 7 & 4 \\ 7 & 4 & 15 \\ 8 & 21 & 6 \end{bmatrix} \tag{25}$$

```
def f_inv(x: np.ndarray):
    print(x)
    A_inv = np.array(
        [
            [15, 7, 4],
            [7, 4, 15],
            [8, 21, 6],
        ]
    )
    b = np.array([1, 2, 3])

    return (A_inv @ (x - b)) % 26

encrypt_word("xsammg", f_inv)
```

This returns `orange` 🍊

6.e)

We want to show that if A is invertible mod m, then $\det A \in (\mathbb{Z}/m\mathbb{Z})^{\times}$.

Proof. Suppose A is invertible mod m. Then $\exists B$ such that $AB = BA = \mathrm{Id}$. From determinant rules:

$$\begin{aligned} \det(AB) &= \det(A)\det(B) = 1 \\ \implies (\det A)^{-1} &= \det(B) \end{aligned} \tag{26}$$

Hence $\det A$ has an inverse mod $m \implies (\det A, m) = 1 \implies \det A \in (\mathbb{Z}/m\mathbb{Z})^{\times}$. $\square$